IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC,	§	
	§	
v.	§	Case No. 2:12-CV-61-JRG-RSP
	§	
WELLS FARGO & CO., et al.,	§	
	§	

CLAIM CONSTRUCTION
MEMORANDUM AND ORDER

After reviewing the arguments set forth in the parties' claim construction briefing (Dkt. Nos. 85, 87, and 94), the Court determined that oral argument on claim construction in the above-captioned case is unnecessary. Dkt. No. 105, 5/10/2013 Order. Upon consideration of the arguments briefed by the parties, the Court issues this Claim Construction Memorandum and Order.

Also before the Court is Defendants' Emergency Motion to Strike Untimely Extrinsic Evidence (Dkt. No. 99), Plaintiff's response (Dkt. No. 104 at Ex. A), and Defendants' reply (Dkt. No. 107).

Table of Contents

BACKGROUND

Plaintiff asserts United States Patent No. 5,412,730 ("the '730 Patent"), titled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995, and bears a priority date of October 6, 1989.

The Court has construed the '730 Patent five times: *TQP Development, LLC v. Merrill Lynch & Co., Inc., et al.*, No. 2:08-CV-471, Dkt. No. 383 (E.D. Tex. Mar. 28, 2011) ("*Merrill Lynch I*"); *id.*, Dkt. No. 512 (May 19, 2012) ("*Merrill Lynch II*"); *TQP Development, LLC v. Barclays PLC, et al.*, No. 2:09-CV-88, Dkt. 165 (E.D. Tex. Mar. 28, 2011) ("*Barclays*"); *TQP Development, LLC v. Ticketmaster Entertainment, Inc.*, No. 2:09-CV-279, Dkt. No. 232 (E.D. Tex. Sept. 23, 2011) ("*Ticketmaster*"); and *TQP Development, LLC v. 1-800-Flowers.com Inc., et al.*, No. 2:11-CV-248 (E.D. Tex. Mar. 20, 2013) ("*1-800-Flowers*").

In general, the '730 Patent relates to secure communication through the use of pseudo-random encryption keys. A sequence of pseudo-random keys is generated based on a seed value and an algorithm, and keys are selected depending upon the message data that is being sent over the transmission medium. The transmitter and receiver are thereby able to generate the same sequence of keys without the security risk of transmitting keys from the transmitter to the receiver or vice versa. The term "pseudo-random" means that the sequence has no apparent regularities unless the seed value and algorithm are known or determined. *Merrill Lynch I* at 23. The Abstract of the '730 Patent states:

> A modem suitable for transmitting encrypted data over voice-grade telephone line. The modem is implemented by the combination of integrated circuit components including a microprocessor, a serial communications controller which communicates with connected data terminal equipment, and a modulator/demodulator for translating between voice band tone signals and digital data. Pseudo random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and a receiving decoder. An initial random number

> seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

The '730 Patent, in its original form, contained one independent claim and one dependent claim. An Ex Parte Reexamination Certificate issued on September 20, 2011, confirming the original claims and adding eight more dependent claims.

Claim 1 of the '730 Patent recites:

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To determine the meaning of the claims, courts start by considering the intrinsic evidence. *See id.* at 1313; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group,* *Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). The intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312-13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314-15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* The specification may also resolve the meaning of ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *accord Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition are entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

In general, prior claim construction proceedings involving the same patents-in-suit are "entitled to reasoned deference under the broad principals of *stare decisis* and the goals articulated by the Supreme Court in *Markman*, even though *stare decisis* may not be applicable *per se*." *Maurice Mitchell Innovations, LP v. Intel Corp.*, No. 2:04-CV-450, 2006 WL 1751779, at *4 (E.D. Tex. June 21, 2006). The Court nonetheless conducts an independent evaluation during claim construction proceedings. *See, e.g.*, *Texas Instruments, Inc. v. Linear Techs. Corp.*, 182 F. Supp. 2d 580, 589-90 (E.D. Tex. 2002); *Burns, Morris & Stewart Ltd. P'ship v. Masonite Int'l Corp.*, 401 F. Supp. 2d 692, 697 (E.D. Tex. 2005); *Orion IP, LLC v. Mercedes-Benz USA, LLC,* 516 F. Supp. 2d 720, 722-735 (E.D. Tex. 2007); *Negotiated Data Solutions, Inc. v. Apple, Inc.*, No. 2:11-CV-390, 2012 WL 6494240 (E.D. Tex. Dec. 13, 2012).

MOTION TO STRIKE

Before the Court is Defendants' Emergency Motion to Strike Untimely Extrinsic Evidence. Dkt. No. 99. Also before the Court are Plaintiff's response (Dkt. No. 104 at Ex. A) and Defendants' reply (Dkt. No. 107).

Defendants requested expedited briefing and resolution of their motion in advance of the then-scheduled May 17, 2013 claim construction hearing. The Court later cancelled that hearing, finding that the claim construction disputes could be resolved on the briefing and without a hearing. Dkt. No. 105, 5/10/2013 Order. The Court therefore addresses Defendants' motion here, in the present Claim Construction Memorandum and Order.

Defendants move to strike the Declaration of Dr. Trent Jaeger, dated April 25, 2013, and filed as an attachment to Plaintiff's Reply Claim Construction Brief (Dkt. No. 94 at Ex. 2). Dkt. No. 99. Plaintiff did not disclose Dr. Jaeger's opinions in the Joint Claim Construction and Prehearing Statement, which is a filing required by Local Patent Rule ("P.R.") 4-3. Plaintiff responds that "[b]ecause [Plaintiff] did not, and could not, foresee Defendants' improper and inconsistent claim construction arguments, [Plaintiff] did not see the need to rebut Defendants' extrinsic evidence and only began to work with Dr. Jaeger on his rebuttal declaration on Monday[,] April 22, 2013, after Defendants served their Defendants' Response Brief on Friday, April 19, 2013." Dkt. No. 104, Ex. A at 1. In particular, Plaintiff points to: "(1) a procedurally improper attempt to challenge the ['730] Patent under 35 U.S.C. 101, under the guise of claim construction, and (2) a challenge to the Court's prior ruling that the applicant for the ['730] patent did not disclaim 'stream ciphers.'" *Id.* at 2.

The Court addressed analogous circumstances in *Lodsys, LLC v. Brother Int'l Corp.*, No. 2:11-cv-90, Dkt. No. 573 (E.D. Tex. Mar. 12, 2013) (Gilstrap, J.). Plaintiff failed to disclose the extrinsic expert opinions of Dr. Jaeger before the start of claim construction briefing, as required by P.R. 4-3(b). Indeed, Plaintiff waited until its Reply Claim Construction Brief to submit a declaration by Dr. Jaeger or to even identify Dr. Jaeger.

Defendants also move to strike an extrinsic dictionary definition of "algorithm" from *The Harper Collins Dictionary of Computer Terms* that Plaintiff attached to its Reply Claim Construction Brief (Dkt. No. 94 at Ex. 1). Dkt. No. 99. Here, too, Plaintiff failed to comply with the disclosure requirements of the Local Patent Rules.

Plaintiff relies upon P.R. 4-5(c) as well as *Syntrix Biosystems, Inc. v. Illumina, Inc.*, No. C10-5870, 2013 WL 496061, 2013 U.S. Dist. LEXIS 17023 (W.D. Wash. Feb. 7, 2013) and *Competitive Technologies v. Fujitsu Ltd.*, 286 F. Supp. 2d 1161 (N.D. Cal. 2003).

Local Patent Rule 4-5(c) states: "Not later than 7 days after service upon it of a responsive brief, the party claiming patent infringement shall serve and file any reply brief and any evidence directly rebutting the supporting evidence contained in an opposing party's response."

Syntrix and *Competitive Technologies* are non-binding authorities and are ultimately unpersuasive in light of the analysis of *Lodsys*, which found that a "wait-and-see" approach to preparing an expert declaration is prohibited by P.R. 4-3. *See* No. 2:11-cv-90, Dkt. No. 573 at 3. Also of note, *Syntrix* relied upon the "rule for disclosure of rebuttal evidence" but provided no analysis, and in *Competitive Technologies* the expert at issue had at least been timely identified. 2013 WL 496061, at *4; 286 F. Supp. 2d at 1168-69. On balance, Plaintiff has failed to demonstrate that the allowance for rebuttal evidence under P.R. 4-5(c) should trump the requirement for disclosure of expert opinions under P.R. 4-3(b). Defendants' motion to strike is therefore granted.

Alternatively, upon review of Dr. Jaeger's declaration and the definition of "algorithm" in *The Harper Collins Dictionary of Computer Terms*, the Court finds that Plaintiff's untimely evidence would not alter the Court's analysis, set forth herein, even if the Court were to deny Defendants' motion to strike.

CONSTRUCTION OF AGREED TERMS

Term	Construction
Preamble	The preamble is limiting and requires: "a method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver"
"data"	No construction necessary
"communications link from a transmitter to a receiver"	No construction necessary
"based on said seed value"	"based exclusively on said seed value"
"associating different ones of seed values with each of a plurality of remote locations with which secured communication is required"	"when secured communication is required with two or more remote locations, associating a different seed value with each of the remote locations"

“associating with each of a plurality of remote locations with which secured communication is required different seed values”	“when secured communication is required with two or more remote locations, associating, at the transmitter, a different seed value with each of the remote locations”
“encrypting the data”	“converting clear text data into cypher text”
“decrypting the data”	“converting cipher text into clear text”
“pseudo-random key values”	“a sequence of numbers that are generated by supplying a seed value to an algorithm, the sequence of numbers have no apparent regularities unless the seed value and algorithm are known or determined”
“said provided seed value is one of a number of seed values for a plurality of remote locations with which secured communication is required”	“when secured communication is required with two or more remote locations, providing more than one seed value for a number of the remote locations for which secured communication is required”

Dkt. No. 85 at 3-4; Dkt. No. 87 at 5-6.

CONSTRUCTION OF DISPUTED TERMS

As a preliminary matter, Plaintiff’s opening brief proposed, without argument, that the Court adopt several of its prior constructions “for consistency.” *See* Dkt. No. 85 at 4. The terms at issue are: (1) “data being transmitted over said link”; (2) “predetermined number of said blocks”; (3) “a new key value in the first sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the transmitter”; and (4) “a new key value in the second sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the receiver.” *Id.* at 4-5.

Plaintiff did not include these terms as disputed terms requiring construction in the Local P.R. 4-3 Joint Claim Construction and Prehearing Statement. *See* Dkt. No. 80 at Ex. B. Likewise, these terms do not appear as distinct disputed terms in the parties P.R. 4-5(d) Joint Claim Construction Chart. *See* Dkt. No. 102 at Ex. A. Because these terms have not been presented to the Court as agreed terms or as disputed terms requiring construction, the Court does not address these terms.

Plaintiff also urges that good cause must be shown for a party to submit a previously construed term for construction. Dkt. No. 85 at 5 (citing *Uniloc USA, Inc. v. Sony Corp. of Am.*, Nos. 6:10-CV-373, -471, -472, -591, -636, -691, 6:11-CV-33, 2011 WL 1980214, at *3, 2011 U.S. Dist. LEXIS 54547, at *31 (E.D. Tex. May 20, 2011)). Such a requirement is not present in the Court's Local Patent Rules, or in any binding authority identified by the parties, and shall not be imposed for the above-captioned case.

Finally, Defendants have argued that to the extent an expert's opinions regarding claim construction are not properly contested by an opposing party's expert, the expert's opinions should be adopted. Dkt. No. 87 at 1 & n.1 (citing *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348 (Fed. Cir. 2013)). The Court is not aware, however, of any authority holding that an expert's opinions should trump the Court's own consideration of all relevant evidence, particularly the intrinsic evidence. *See Phillips*, 415 F.3d at 1318 ("[A] court should discount any expert testimony that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent.") (internal quotation marks omitted).

A. "predetermined"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary Alternatively: "determined before any communication of a sequence of encrypted blocks"	"determined before any communication over the communication link, but not an inherent property of the encryption or key-generation algorithms"

Dkt. No. 102, Ex. A at 1.

<u>(1) The Parties' Positions</u>

Plaintiff argues that "[t]he term 'predetermined' is a commonly used term and does not need any construction" and "simply means to determine beforehand." Dkt. No. 85 at 11 (citing

Ex. F, *Merriam-Webster Dictionary* (on-line version)). Alternatively, Plaintiff proposes the construction adopted by the Court in *1-800-Flowers*. *See 1-800-Flowers* at 34. Plaintiff urges that Defendants' proposal would improperly narrow the claims in situations, for example, where unencrypted data is transmitted before any encrypted data is transmitted. *Id.* at 12. Plaintiff further argues that Defendants' proposal to exclude "an inherent property of the encryption or key-generation algorithms" is ambiguous and confusing and has "no basis in the claims, specification or intrinsic record." *Id.*

Defendants respond that Plaintiff is attempting to recapture what Plaintiff distinguished during prosecution, namely the prior art "stream cipher" techniques that involve "producing a new pseudo-random 'key' value (based on a seed) to encrypt each unit of data." Dkt. No. 87 at 6. Defendants submit that if such prior art techniques were found to be within the claim scope, then Claim 1 is invalid. Defendants also urge that because the term "predetermined" was added during prosecution, that term must carry some meaning, to wit, "determined before." *Id.* at 7 (internal quotation marks omitted). Defendants further argue that the predetermined values cannot be inherent properties of the algorithms because the specification explains that the values are "not known to would-be attackers." *Id.* at 7-8. Defendants emphasize that the prior art stream ciphers involved changing to a new key value for each data unit and therefore did not involve any "predetermined" interval. *Id.* at 8; *see* Dkt. No. 80, Ex. D, Franklin Decl., *e.g.*, at ¶ 36.

Plaintiff replies that "predetermined" is unambiguous and that no prosecution disclaimer occurred because "the applicant simply complied with the Examiner's unexplained instructions to rewrite application claim 8 with the limitations of application claims 9 and 10." Dkt. No. 94 at 3. Plaintiff also reiterates that Defendants' proposal is ambiguous. *Id.* at 4-5.

(2) Analysis

Although Plaintiff argues that this term should not be construed, the briefing demonstrates that the parties have a "fundamental dispute regarding the scope of a claim term," and the Court has a duty to resolve the dispute. *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362-63 (Fed. Cir. 2008).

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a *predetermined* characteristic of the data being transmitted over said link,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said *predetermined* characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] a new one of said key values in said first and said second sequences being produced each time a *predetermined* number of said blocks are transmitted over said link, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

Defendants have relied upon prosecution history concerning the "Feistel" reference, United States Patent No. 4,316,055. "[T]he prosecution history (or file wrapper) limits the interpretation of claims so as to exclude any interpretation that may have been disclaimed or disavowed during prosecution in order to obtain claim allowance." *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985). In *Barclays*, this Court considered and rejected the same argument. *Barclays* at 13-14. The Court reaches the same conclusion here and finds no definitive statements by the patentee that would warrant a finding of prosecution disclaimer. *Omega Eng. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added).

Nonetheless, the specification discloses that for encryption and decryption to occur, certain information must be provided to the transmitter and the receiver "in advance":

> In accordance with the invention, to permit the two stations to communicate, each [is] *supplied in advance* with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.
>
> The monitoring function can advantageously be performed simply by counting the units of data being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number. In this way, no additional synchronization information needs to be added to the data stream.

'730 Patent at 1:43-59 (emphasis added).

> *Once the host station has supplied the initial seed value keys to the units forming the two terminal locations for a given link and transmission over that link begins*, the host . . . no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host.

Id. at 2:17-25 (emphasis added).

> Of course, in order for the receiving station to successfully decipher the incoming cipher text, the receiving station 12 must be provided (in some fashion) with both the correct seed value and the correct interval number. *These values are supplied to the receiving station in advance of the transmission by any secure means.*

Id. at 4:13-20.

As found in *Ticketmaster*, these disclosures, as well as the plain language of the claim, are consistent with construing "predetermined" to refer to a determination that occurs before any communication involving data comprising a sequence of blocks that have been encrypted using the recited pseudo-random key values. Otherwise, the recited sequences of pseudo-random keys could not be produced and, in turn, the data could not be encrypted.

Finally, Defendants' have cited the Court's analysis in *Calypso Wireless, Inc. v. T-Mobile USA Inc.*, No. 2:08-CV-441, Dkt. No. 309 (E.D. Tex. Jan. 15, 2013). In *Calypso*, the Court addressed whether the term "predetermined, maximum distance" could refer to the range inherent in any wireless system. *Calypso* involved a different patent and different technical issues. On balance, the Court's analysis in *Calypso* is not relevant to construing the term "predetermined" in the above-captioned case and does not warrant importing a limitation that "predetermined" excludes any and all "inherent propert[ies] of the encryption or key-generation algorithms," as Defendants have proposed.

The Court therefore hereby construes **"predetermined"** to mean **"determined before any communication of a sequence of encrypted blocks."**

B. "a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link"

Plaintiff's Proposed Construction	Defendants' Proposed Construction
"a new key value in the first and second sequence is produced each time a predetermined number of blocks are transmitted over the link" Alternatively: "a new key value in the first and second sequence is *used* each time a predetermined number of blocks are transmitted over the link"	"using a new key value in each sequence each time the transmitter transmits a predetermined (and pre-supplied) number of blocks over the link to the receiver, and only at those times"

Dkt. No. 102, Ex. A at 1; Dkt. No. 85 at 6 (emphasis modified).

(1) The Parties' Positions

Plaintiff argues that its proposals are appropriate for distinguishing the times when key values are generated from the times when key values are "advanced and applied to the data to perform encryption and decryption." Dkt. No. 85 at 6. Plaintiff submits that "Defendants' proposed construction improperly changes 'are transmitted' to 'transmits' and imports a temporal limitation requiring the receiver to use a new key value at the moment the transmitter sends the predetermined number of blocks—but before the predetermined number of blocks may be received by the receiver—'and only at this time'." *Id.* at 7. Plaintiff counters that in one disclosed embodiment, synchronization is maintained "by employing means at both the transmitter and receiver to monitor the flow of data and advance the keys." '730 Patent at 3:48-53. Finally, Plaintiff argues that the term "pre-supplied" in Defendants' proposal is ambiguous because "[i]t is unclear whether 'pre-supplied' is intended to modify the new key values, the predetermined number of blocks, or the number of transmitted blocks." Dkt. No. 85 at 7.

Defendants respond:

> First, Defendants' construction, but not [Plaintiff's], makes clear that the only time at which a new key value is used is when the predetermined number of blocks has been transmitted. Second, Defendants' construction clarifies that "produced" refers to use of the key. Third, Defendants' construction seeks to make clearer the causal relationship between the two actions recited in this claim language: namely, the act of transmitting the predetermined number of blocks is what triggers the act of using the next new key value.

Dkt. No. 87 at 11. Defendants further argue that "the claim language expressly confirms that the new key value must be produced when data blocks 'are transmitted.'" *Id.* Likewise, Defendants argue, "use of the past tense 'transmitted' in the claim indicates that the transmitter does not switch to the next key until after the predetermined number of data blocks have been transmitted, which refutes [Plaintiff's] proposed construction." *Id.* at 12. Finally, Defendants argue that "the number of blocks must be provided before the initial handshake process between a transmitter and receiver." *Id.* (citing '730 Patent at 10:48-59). Defendants urge that Plaintiff should not be permitted to disavow the limitation, relied upon during prosecution, in which the claim "conditions a key switch on the transmission of a predetermined number of blocks." *Id.* at 14.

Plaintiff replies that Defendants' proposed "temporal limitation must be rejected because it reads 'transmitted over said link' out of the claim, *i.e.*, the key values would advance at the moment the blocks leave the transmitter but before the blocks reach the endpoint of the communication link." Dkt. No. 94 at 5. As to the prosecution history, Plaintiff replies that "the distinction drawn between Maisel [(a prior art reference)] and the ['730] patent does not support Defendants' temporal limitation because the receiver would not advance the encryption key until it receives the advance signal, *i.e.*, which is not necessarily at the moment the blocks are transmitted." *Id.* at 6.

(2) Analysis

Claim 1 recites (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another[,] *a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link*, and

> decrypting the data sent over said link at said receiver in accordance with said second sequence.

In *Barclays*, the Court agreed with Plaintiff's argument that "what is important is that each key be *used* at precisely the right time relative to the data. It does not matter whether that key is generated at that time, or pre-generated and stored." *Barclays* at 16; *see id.* at 17. *Barclays* construed the disputed term to mean "a new key value in the first and second sequence is produced each time a predetermined number of blocks are transmitted over the link." *Id.* at 18.

The Abstract of the '730 Patent states (emphasis added):

> The *random number generators are advanced* at times determined by predetermined characteristics of the data being transmitted so that, *after transmission has taken place*, the common encryption key can be known only to the transmitting and receiving stations.

The specification discloses counting blocks to determine when to advance to a new key value:

> In accordance with a principle feature of the present invention, pseudo-random number generators are employed at both the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. *In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.*
>
> The monitoring function can advantageously be performed simply by *counting the units of data being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number*. In this way, no additional synchronization information needs to be added to the data stream. For even greater security, the interval number (which must be reached before the key is switched) may itself be a changing value generated by a random number generator, so that the duration during which a given key is active changes from key to key at times which are predictable only by the authorized recipient.

'730 Patent at 1:37-65 (emphasis added).

> The advance signal produced by block counter 21 is supplied to the advance input of a pseudo-random number generator 23 which *supplies a sequence of encryption key values to the key input of the encryptor 17*. The content of the key sequence is predetermined by the combination of (1) the internal makeup of the generator 23 and by (2) a supplied random number seed value which initializes the generator 23. *The generator 23 responds to each advance signal from block counter 21 by changing its output to the next successive encryption key value.* Thus, for example, the combination of counter 21 and generator 23 operate to *change the encryption key each time* [*the*] *total number of bytes transmitted is an exact multiple of the predetermined interval number*.
>
> * * *
>
> The block counter 21 need not supply advance signals on boundaries between encryption units, nor does the generator 23 need to provide [the] new key value precisely on encryption unit boundaries. Instead, the encryptor 17 may *buffer the new key*[] *temporarily*, using it for the first time on the next successive encryption unit of data.
>
> * * *
>
> *Block counter 29* performs the identical function as that performed by the counter 21 at the transmitting station 11 and hence *supplies advance signals to the generator 27 at precisely the same times (relative to the data stream) that counter 21 advances generator 23*. Each time the current count reaches the interval number, the pseudo-random number generator 27 is advanced. Since the internal makeup of random number generator 27 is identical to that of generator 23, and since it is supplied with the same seed value, and since block counter 29 is supplied with the same interval number value as that supplied to the block counter 21, exactly the same sequence of keys will be supplied to the random number generators 23 and 27, and *the keys will change at precisely the same time* (relative to the data stream) to accurately decipher the transmitted data.

Id. at 3:26-40, 3:50-56 & 3:64-4:12 (emphasis added).

Defendants have also relied upon prosecution history involving the "Maisel" reference, WO 87/00377, in which the patentee explained:

> Thus, the "time" in claim 1 is not a chronological time (such as 3:51 PM, or such as 34 seconds), but rather [is] a shorthand way of referring to the satisfaction of a condition, i.e., one that is dependent upon a predetermined characteristic of the data being transmitted. One example of such a satisfied condition is provided at [the '730 Patent at] 3:19-25, which is satisfied when the block counter counts a certain number of blocks (an "interval number") being transmitted.

Dkt. No. 87, Ex. P, 5/18/2011 Response Under 37 CFR 1.111 and Proposed Amendment Under 37 CFR 1.530 at 6.

Thus, the ‘730 Patent refers to “a sequence of encryption key values” and also to “advanc[ing] the random number generator,” when a certain number of data units have been transmitted, so as to use a new encryption key. *See id.* at Abstract, 1:37-65 & 3:26-40. As found in *Barclays*, Claim 1 does not specify whether the key is generated at the time of use or is generated ahead of time and then selected at the time of use. *Barclays* at 17 (“The claim further only requires that each new key be ‘produced’ at a specific time relative to the data. It does not matter whether that key is generated at that time, or pre-generated and stored.”). To whatever extent Defendants are proposing that the new key value cannot be created until after the predetermined number of blocks have been transmitted, Defendants’ proposal is hereby expressly rejected.

Finally, as to the determination of whether “a predetermined number of said blocks” have been “transmitted over said link,” the claim explicitly refers to transmission, not to encryption or to some other step of preparing for transmission. Defendants’ proposal of the phrase “only at those times” is superfluous and confusing and should therefore be omitted from the Court’s construction. Instead, the Court’s construction should reflect that a new key value is used each time a predetermined number of blocks have been sent.

The Court accordingly hereby construes **“a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link”** to mean **“a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent from the transmitter over the communication link.”**

C. “seed value”

Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
No construction necessary	“the supplied value which initializes the generating of the pseudo-random numbers”

Dkt. No. 102, Ex. A at 1-2.

(1) The Parties’ Positions

Plaintiff argues that “[t]he term ‘seed value’ requires no construction because the meaning of this term is made clear by the claims themselves and the specification.” Dkt. No. 85 at 13.

Defendants respond:

> Defendants submit that the seed value is a value which **initializes** the generating of the pseudo-random key values, and is a value that exists **prior to** communications taking place over a communication link. Defendants also submit that the “seed value” is **provided to** or **supplied to** the random number generators **by different secured links**, and not shared back and forth or independently created by the transmitter and receiver.

Dkt. No. 87 at 15. Defendants further submit that in Plaintiff’s infringement contentions, Plaintiff has interpreted “seed value” to encompass “a value that is **calculated** by both the transmitter and receiver through iterative steps over the communication link instead of being provided to them.” *Id.* Defendants explain that the seed value cannot be created during encrypted communications because the key values used for encryption are generated based on the seed value. *Id.* at 17. Defendants further urge that the specification consistently uses the term “seed value” to refer to an “initial” value that is provided in advance. *Id.* at 17-18.

Plaintiff replies that “[t]here is nothing confusing or ambiguous about what a ‘seed value’ is or what the ‘seed value’ does, and there is no reason to construe this claim [term].” Dkt. No. 94 at 7.

<u>(2) Analysis</u>

Although Plaintiff argues that this term should not be construed, the briefing demonstrates that the parties have a "fundamental dispute regarding the scope of a claim term," and the Court has a duty to resolve the dispute. *O2 Micro*, 521 F.3d at 1362-63.

Claim 1 recites, in relevant part (emphasis added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a *seed value* to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said *seed value* at said transmitter, . . .
>
> generating a second sequence of pseudo-random key values based on said *seed value* at said receiver, ...

The Abstract of the '730 Patent states that "[a]n initial random number seed value is made available to both [the transmitting and receiving] stations." The specification discloses "seed values" multiple times:

> In accordance with a principle feature of the present invention, pseudo-random number generators are employed at both the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a *random number seed value* which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators.

'730 Patent at 1:37-48 (emphasis added).

> Once the host station has supplied the *initial seed value keys* to the units forming the two terminal locations for a given link and transmission over that link begins, the host . . . no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host.

Id. at 2:17-25 (emphasis added).

> *The random number generators 23 and 38 at the transmitting station obtain their seed values from a key memory 50*. Key memory 50 stores the *random number*

> *keys* indexed by destination (along with telephone dial-up numbers for automatic dialing). Similarly, at the receiving station, *the seed values for the remote terminals from which the receiving station is authorized to receive information are stored in a key memory 60 connected to supply seed values to the generators 27 and 40.* The key memories eliminate[] the need for authorized users to remember and enter *keys* before each transmission or reception.

Id. at 9:51-62 (emphasis added).

> [K]nowledge of the *initial seed values* supplied by the host are of no further value and cannot be used to monitor ongoing communications over the authorized link.

Id. at 11:5-8 (emphasis added).

The claim language and the above-quoted portions of the specification are consistent with Defendants' argument that the "seed value" is provided in advance of key generation and, therefore, is not created as part of the claimed key generation process. Any other interpretation would read the word "seed" out of the claim. Nonetheless, Plaintiff properly submits that unencrypted communication could precede encrypted communication and, as a result, the seed value might not necessarily exist prior to *any* communications taking place over the communication link. Thus, the plain meaning of "seed value" is appropriate, but the Court provides additional explanation, as follows:

The Court hereby construes **"seed value"** to have its **plain meaning**. The Court further hereby finds, as part of its construction: **"The seed value is provided to the transmitter prior to generating the first sequence of pseudo-random key values, and the seed value is provided to the receiver prior to generating the second sequence of pseudo-random key values."**

D. "providing a seed value to both said transmitter and receiver"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"providing the same seed value to both the transmitter and receiver"	"providing the same seed value to both the transmitter and receiver from different secured links"

Dkt. No. 102, Ex. A at 2.

(1) The Parties' Positions

Plaintiff argues that "the claims do not place any restriction on where the seed originates or how it is provided." Dkt. No. 85 at 8. To the contrary, Plaintiff cites disclosure that "the seed values can be provided 'by any secure means'" and can be generated and provided locally. *Id.* (citing '730 Patent at 4:13-19 & 10:23-34).

Defendants respond that the use of different terms, "providing" and "generating," implies a difference in meaning. Dkt. No. 87 at 18. Defendants also argue that because the claim language recites providing a seed value "to both said transmitter and receiver," "[n]either can 'provide' the seed value to itself." *Id.* at 19. In other words, "[b]ecause a seed value cannot be both internally generated at one end and 'provided to both' ends, the source of the seed value, according to the plain language of the claim, must be external to the transmitter and receiver." *Id.*

As to Figure 4 of the '730 Patent, Defendants submit that even though key values are obtained from key memories within the transmitter and receiver, those values were provided from an external source. *Id.* at 19-20.

Plaintiff replies by emphasizing that it proposes the construction reached in *Merrill Lynch I* and *Ticketmaster*. Dkt. No. 94 at 8. Plaintiff also argues that "Figure 4 does not show a seed value being provided from an external source and the specification explicitly states that the seed values can be provided 'by any secure means' and teaches loading the key memories by local command." *Id.* Finally, Plaintiff submits that "the claims themselves distinguish between 'providing' and 'generating,' and a jury can readily understand what the difference is between 'providing' and 'generating.'" *Id.* at 9.

(2) Analysis

In *Merrill Lynch I*, the Court noted the disclosure, with reference to Figure 4 of the ‘730 Patent, that seed values could be obtained from “key memory 50” within “transmitting station 11” and from “key memory 60” within “receiving station 12.” *Merrill Lynch I* at 18-19. In *Ticketmaster*, the Court found that “[a]lthough[] the transmitter would be required to have the seed value to generate the encryption keys prior to transmission, there is no explicit requirement in the patent or file history that suggests that the receiver must also be provided the seed value prior to transmission.” *Ticketmaster* at 9; *see id.* at 12. *Ticketmaster* found, instead, that “[t]he invention of the ‘730 patent would likewise function if the seed value was provided to the receiver any time prior to decrypting the encrypted data sent over the link.” *Id.* at 9; *see id.* at 12.

The specification discloses that the transmitter and receiver must be provided with the seed value in order to perform their respective functions:

> In accordance with the invention, to permit the two stations to communicate, each [is] supplied in advance with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators. In order that the two generators switch from one output key value to the next in synchronism, means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition.

‘730 Patent at 1:43-53.

> Once the host station has supplied the initial seed value keys to the units forming the two terminal locations for a given link and transmission over that link begins, the host . . . no longer “knows” the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an “insider” who is in possession of the initial key values supplied by the host.

Id. at 2:17-25.

> Of course, in order for the receiving station to successfully decipher the incoming cipher text, the receiving station 12 must be provided (in some fashion) with both

> the correct seed value and the correct interval number. These values are supplied to the receiving station in advance of the transmission by any secure means.

Id. at 4:13-20.

> Data signals from the DTE [(data terminal equipment)] which are to be transmitted are encrypted as described above and shown in FIG. 1, the random number seed values and the interval number values being pre-supplied to the microprocessor 101 and stored in memory subsystem 103.

Id. at 5:15-19.

> The random number generators 23 and 38 at the transmitting station obtain their seed values from a key memory 50. Key memory 50 stores the random number keys indexed by destination (along with telephone dial-up numbers for automatic dialing). Similarly, at the receiving station, the seed values for the remote terminals from which the receiving station is authorized to receive information are stored in a key memory 60 connected to supply seed values to the generators 27 and 40. The key memories eliminate[] the need for authorized users to remember and enter keys before each transmission or reception.
>
> In addition, the use of key memories allows the stations to be operated as terminals in a secure network under the control of a central station which, in separate transmissions over different secure links, enters (and erases) the keys needed by authorizing sending and receiving stations connected to the network.

Id. at 9:51-68.

> A switch operated by a physical key is also advantageously included in each station unit and has "security enabled" and "security disabled" positions. The key memory can only be loaded with values identifying one or more remote units with whom communications are authorized when the switch is in the "security disabled" position (typically when the unit is being set up by an authorized operator who has the physical key needed to disable the security switch). At that time, the table can be loaded either from a remote (host) station or by a local command which takes the form of an extension to the standard modem AT command set. That load command take[s] the form:
>
> AT JSN KDESKEY PHONENUM
>
> where AT is the AT command prefix, JSN is the letter "J" immediately followed by the serial number of the remote station with which communications is authorized, KDESKEY is the letter "K" immediately followed by an 8 character DES encryption key, and PHONENUM is the standard routing code (e.g. dial-up phone number string). In the preferred embodiment, up to 1000 serial numbers and keys, and up to 100 optional dial-up phone number strings (each with up to 39 digits) may [be] stored in the key memory lookup table.

Id. at 10:21-46.

> In accordance with an important feature of this arrangement, the host system may initially authorize communication between two connected units by supplying the appropriate serial numbers and initial key values (unique to an authorized link), but as soon as transmission begins between the two units over the authorized link, the encryption keys are changed in ways that are unknowable to the host. As a consequence, knowledge of the initial seed values supplied by the host are of no further value and cannot be used to monitor ongoing communications over the authorized link.

Id. at 10:66-11:8.

Figures 1 and 4 of the '730 Patent are reproduced here:

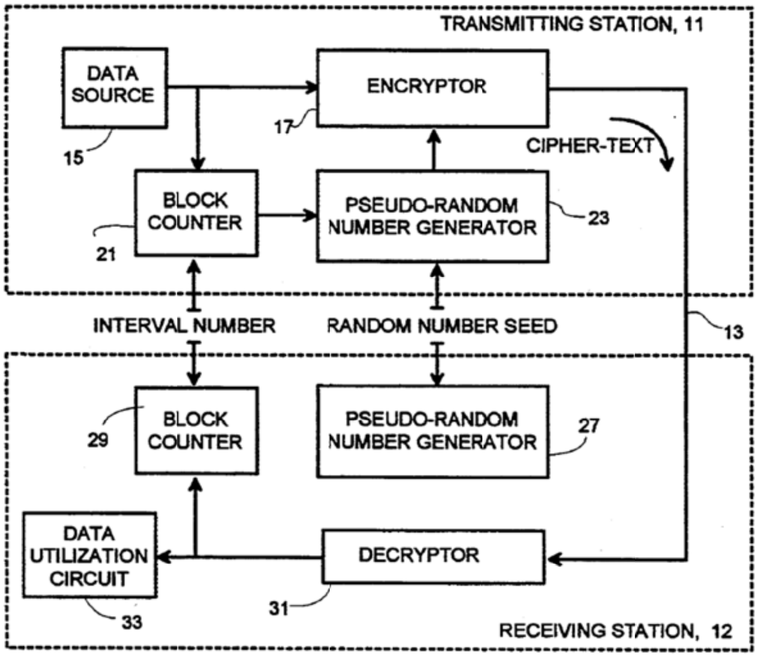

Fig. 1

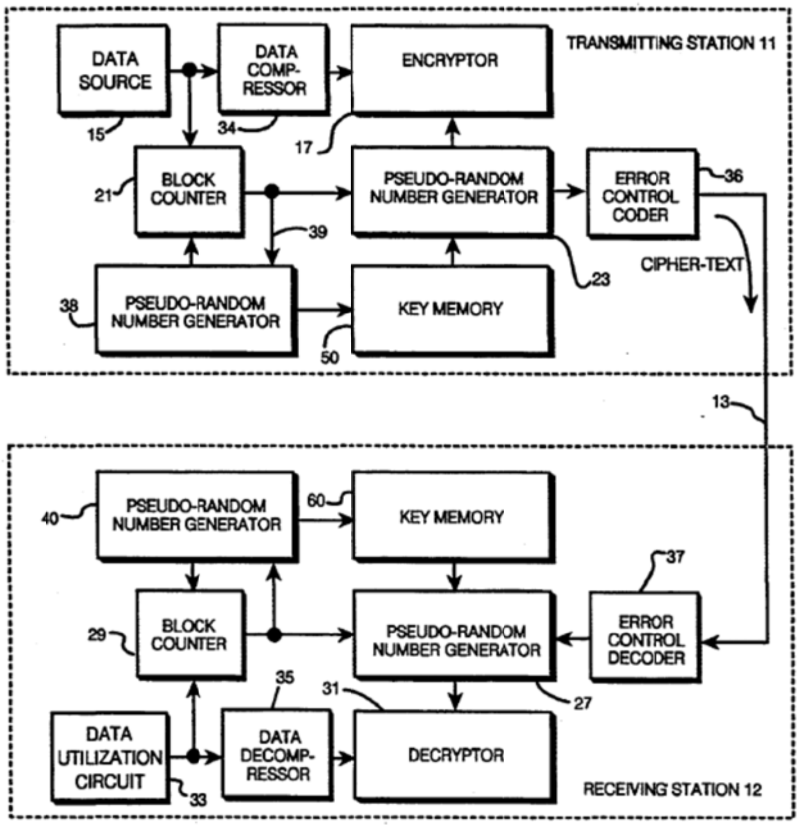

Fig. 4

Defendants also submit that during prosecution, the patent examiner distinguished "providing" from "generat[ing]":

> Lee et al ('027); Weldon, Jr. ('246); and, Feistel ('055) all show systems that use pseudorandom sequences to encrypt and decrypt the data sent between the two communicating parties. It is noted that the language in claim 8 does not link the provision of the "seed value" to the transmitter and the provision of the "seed value" to the receiver. Further, it is noted that "providing" does not indicate that the "seed value" is generated. Please note in section 4.1 of Primality and Cryptography by Evangelos Kranakis that the use of seed values is inherent in pseudorandom number generators.

Dkt. No. 87, Ex. C, 7/8/1993 Office Action at 2.

On balance, Defendants have failed to justify their proposed limitation that the seed value must be provided to both the transmitter and the receiver "from different secured links." The claim language does not recite separate sources or links. Further, Defendants have not shown that the claimed use of a pseudo-random sequence of encryption keys necessarily precludes the seed value from being provided by the transmitter or the receiver. In short, the origin of the seed value is not a limitation of the claim. Nothing in the specification or the prosecution history demands otherwise. Defendants' proposal to limit the claims to a preferred embodiment is hereby expressly rejected. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323.

The Court therefore hereby construes **"providing a seed value to both said transmitter and receiver"** to mean **"providing the same seed value to both the transmitter and receiver."**

E. "block"

Plaintiff's Proposed Construction	Defendants' Proposed Construction
"a group of bits, such as a character, word, or other unit of data"	"a group of bits longer than a byte (in encrypted form)[1]

Dkt. No. 102, Ex. A at 2 & n.1.

<u>(1) The Parties' Positions</u>

Plaintiff proposes the construction reached by the Court in *Merrill Lynch I*. *Merrill Lynch I* at 16. Plaintiff submits that the term "block" is not defined in the patent and that neither the claim language nor the specification places any restriction on block size. Dkt. No. 85 at 10.

Defendants respond that "the 'such as' and 'other unit of data' portions of its construction render the scope of the claim indefinite." Dkt. No. 87 at 21. Defendants also argue that the patentee "disclaimed and distinguished his claimed method over stream cipher systems that encrypt by single byte." *Id.* Further, Defendants explain, "the block counter would be

[1] Defendants would have agreed to drop the "(in encrypted form)" portion of their construction if Plaintiff had agreed that "said blocks" recited in claim 1 are "in encrypted form" consistent with the recitation of "blocks in encrypted form" in the preamble. Defendants submit that Plaintiff did not respond to that proposal. Dkt. No. 102, Ex. A at 2 & n.1.

unnecessary if the encryption key were changed for each character." *Id.* at 23; *see* Dkt. No. 80, Ex. D, Franklin Decl., *e.g.*, at ¶¶ 30-31. Defendants also submit:

> [T]he specification states that the block counter may count the length of the data stream in byte units, in larger word units, "**<u>or</u>**" in block units. (*Id.* at 3:16-25 (emphasis added).) The general grammatical construction of such a disjunctive list of items separated by commas and a concluding "or" is that the listed items are alternatives to each other. *See, e.g., Quindlen v. Prudential Ins. Co.*, 482 F.2d 876, 878 (5th Cir. 1973).

Id.

Plaintiff replies that "there was no clear and unambiguous disclaimer of stream ciphers in the prosecution history, and the Court should reject Defendants' attempt to read a limitation into the term 'block' based on Professor Franklin's [(Defendants' expert's)] opinion that the prosecution history 'suggests' that the claims of the ['730] patent were amended to distinguish well-known 'stream cipher' technology." Dkt. No. 94 at 9.

<u>(2) Analysis</u>

As the Court stated in *Merrill Lynch I*, "the specification does not provide an explicit definition of the term 'blocks.'" *Merrill Lynch I* at 10; *see id.* at 12. As to the prosecution history, *Merrill Lynch I* noted: "The Court agrees that the applicant did limit the term 'data.' However, what is unclear from the prosecution history is exactly how the term 'data' was narrowed by the amendment." *Id.* at 13. *Merrill Lynch I* found that "contrary to Defendants' contention, it is unclear from the intrinsic record if the only defining feature of a block with which to narrow the term 'data' is length." *Id.* at 14 (internal citation and quotation marks omitted). Having considered the intrinsic evidence as well as extrinsic definitions submitted by the parties, *Merrill Lynch I* concluded that rather than specifying any particular length, "the term 'block' narrowed the term 'data' by requiring the data to be a group of bits, such as a character, word, or other unit of data." *Id.* at 16.

The specification discloses various different groupings of data, and those groupings may indeed be fixed-length:

> The monitoring function can advantageously be performed simply by counting the *units of data* being transmitted and by advancing each pseudo-random key generator each time the count reaches an agreed-upon interval number.

‘730 Patent at 1:54-58 (emphasis added).

> *The data from source 15 may take substantially any form, such as a file of text characters, each encoded as a 8-bit byte, or a file of numerical binary information expressed in 16-bit or 32-bit words.* A block counter 21 monitors the stream of data from the source 15 and generates an “advance signal” each time the data meets a predetermined condition. Advantageously, the block counter 21 may simply count the number of bytes (characters), words or blocks of data being transmitted, compare the current count with a predetermined 37 [“]interval number” and produce an advance signal each time the current count reaches the interval number (at which time the current count is reset to 0).

Id. at 3:13-25 (emphasis added).

> *The encryptor 17 translates fixed length segments of the data from source 15 (“clear text”) into fixed-length “cipher text” output segments*, each segment translation taking place in a manner uniquely determined by the encryption key currently supplied by the pseudo-random number generator 23.

Id. at 3:41-46 (emphasis added).

> Note also that, as depicted in FIG. 4, the data is monitored by the block counter 21 prior to compression, rather than afterwards. Correspondingly, at the receiving station 12, the block counter 29 monitors the data flow after it is decompressed. In this way, both counters monitor the same data stream. Both could be reconnected to monitor the compressed data stream if desired, however.

Id. at 9:12-19.

On balance, the claimed invention depends upon the transmitter and receiver counting blocks in the same manner, but nothing in the ‘730 Patent requires that the blocks must be fixed-length or of any particular length. The above-quoted discussion of fixed-length segments and of segments longer than one byte thus relates to a preferred embodiment. Defendants’ expert’s opinion that a block must include more than a single byte is unpersuasive. *See* Dkt. No. 80, Ex.

D, Franklin Decl., *e.g.*, at ¶¶ 39. As found in *Merrill Lynch I*, the patentee made no disclaimer in this regard. *See Merrill Lynch I* at 12-16. Thus, Defendants' proposal would improperly import a limitation into the claims and is hereby expressly rejected. *Comark Commc'ns*, 156 F.3d at 1187; *accord Phillips*, 415 F.3d at 1323.

The Court therefore hereby construes **"block"** to mean **"a group of bits, such as a character, word, or other unit of data."**

F. "sequence of blocks in encrypted form"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary Alternatively: "a sequence of two or more blocks that have been encrypted"	"sequence of two or more blocks that have been encrypted using the same key value"

Dkt. No. 85 at 13.

Defendants present no argument on this term, and this term does not appear in the parties' post-briefing Joint Claim Construction Chart. *See* Dkt. No. 87; *see also* Dkt. No. 102 at Ex. A. Also, in the parties' pre-briefing Joint Claim Construction and Prehearing Statement, Defendants submitted that they "contend that no construction of [sequence of blocks] is necessary in view of constructions proffered" for other terms. Dkt. No. 80, Ex. C at 14-15. The Court concludes that this term is not disputed and, therefore, the Court need not construe this term.

G. "transmitter," "receiver," and "each of the asserted claims as a whole"

"transmitter" and "receiver"	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	Ordinary meaning

“each of the asserted claims as a whole”	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
No construction necessary	“does not require any particular machine or any particular transformation of any particular article”

Dkt. No. 102, Ex. A at 3.

(1) The Parties’ Positions

Plaintiff argues that because Defendants have cited extrinsic evidence that defines “transmitter” and “receiver” in terms of a “person,” Defendants’ proposals should be rejected. Dkt. No. 85 at 15. Plaintiff notes that “the specification does not describe a person performing various steps of an encryption and transmission process; instead, it extensively describes an electronic system, including block diagrams, connection diagrams, and source code, for transmitting encrypted data.” *Id.* at 16.

As to the claims as a whole, Plaintiff argues that Defendants are improperly seeking summary judgment of invalidity, under 35 U.S.C. § 101, arguing that the claims are directed to an unpatentable mathematical formula or mental process. *Id.* at 17. Alternatively, Plaintiff argues that the claimed subject matter is not abstract and instead is tied to particular equipment and transformative processes.

Defendants respond that they do not seek summary judgment of invalidity in the course of these claim construction proceedings, but Defendants submit that the underlying issue of whether the claims are tied to a particular machine is an issue of claim construction. Dkt. No. 87 at 24. Defendants explain, “The claims do recite where the mathematical operations are performed, namely ‘at’ the transmitter or receiver end of the communication link. This is part of the algorithm. But, the claims do not recite what performs these operations.” *Id.* at 25. As to "transmitter" and "receiver," Defendants conclude that "the Court should give these terms their ordinary meaning—which is not restricted to a particular machine." *Id.* at 26.

As to the claims as a whole, Defendants argue that "[a]s is true for 'transmitter' and 'receiver,' nothing else restricts these claims to a particular machine performing the method." *Id.*

Plaintiff replies:

> Despite their agreement to the plain meaning of these claim terms, Defendants set forth an erroneous definition of "transmitter" and "receiver" which make no sense in the context of the claims: that "***anything*** capable of transmitting or receiving data" includes "***a person or thing*** that transmits something." . . . One of ordinary skill in the art would understand that a "person" is not being referred to as the claimed "transmitter" and "receiver."

Dkt. No. 94 at 10. As to the claims as a whole, Plaintiff replies: "[T]he fact that the claims of the ['730] patent make use of machines, including a transmitter, receiver, and communication link to accomplish a novel method for key management and encryption[,] is all that is required for the invention to be patentable." *Id.* at 12.

(2) Analysis

On one hand, as Defendants submit, claim construction can be "an important first step in a § 101 analysis." *In re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008) (en banc), *aff'd sub nom. on other grounds, Bilski v. Kappos*, 130 S. Ct. 3218 (2010); *see also Power Mosfet Techs., LLC v. Siemens AG*, 378 F.3d 1396, 1404, 1410, 1412 (Fed. Cir. 2004) (noting that terms "were construed in isolation, and at no other time did the district court or the Special Master construe the claims as a whole. . . . [C]onstruction of the claims as a whole would have been beneficial").

On the other hand, Defendants' arguments regarding whether the claims are tied to a particular machine or to a particular transformation are arguments on the ultimate issue of whether the claims are directed to patentable subject matter. *See generally Bilski v. Kappos*, 130

S. Ct. 3218. The dispute in *Power Mosfet* was far more specific, involving a dispute as to whether an "interface" "encompasse[d] both a 2-D surface and 3-D structures or areas." 378 F.3d at 1410-11.

On balance, Defendants' validity arguments as to "transmitter," "receiver," and the claims as a whole would be more properly addressed in the context of a motion for summary judgment rather than as part of claim construction. *Phillips*, 415 F.3d at 1327 ("[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction."). The Court accordingly hereby construes **"transmitter"** and **"receiver"** to have their **plain meaning**, and the Court hereby expressly rejects Defendants' proposal to construe "each of the asserted claims as a whole."

H. "compressing the data prior to encrypting the data"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary	"applying a compression function to all of the data to reduce the size of the data to be encrypted and transmitted"

Dkt. No. 102, Ex. A at 7.

<u>(1) The Parties' Positions</u>

Plaintiff argues that Defendants' proposal would improperly limit the claim to applying a *single* compression function and to compressing *all* of the data. Dkt. No. 85 at 17.

Defendants respond that "[a] word or phrase used consistently throughout a patent claim should be interpreted consistently." Dkt. No. 87 at 28 (quoting *Phonometrics, Inc. v. N. Telecom, Inc.*, 133 F.3d 1459, 1465 (Fed. Cir. 1998)). Defendants argue that "[a]fter independent claim 1 introduces a method for transmitting encrypted 'data', additional references to '**the** data' should be construed to refer back to the same data that is encrypted and transmitted, not just some of that data." *Id.* at 28-29. Finally, Defendants respond that their proposal does *not* require a *single* function but rather merely "a compression function." *Id.* at 29.

Plaintiff replies:

> One of ordinary skill in the art would understand that "the data" being compressed prior to encryption in claim 10, is "the data" referred to in claim step 1.b. The extraneous language of Defendants' proposed construction does nothing to clarify this relationship and improperly adds limitations.

Dkt. No. 94 at 13-14.

(2) Analysis

The disputed term appears in Claim 10. Claim 10 depends from Claim 9, which is a multiple dependent claim that depends from Claims 3, 4, 5, 6, 7, and 8. Those claims, in turn, all ultimately depend from Claim 1. The antecedent basis for "the data" in the disputed term in Claim 10 appears in Claim 1. Claims 1, 9, and 10 recite (emphasis added):

> 1. A method for transmitting *data* comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the *data* being transmitted over said link,
>
> encrypting the *data* sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said *data* transmitted over said link such that said first and second sequences are identical to one another[,] a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link, and
>
> decrypting the *data* sent over said link at said receiver in accordance with said second sequence.
>
> * * *
>
> 9. The method of any one of claims 3, 4, 5, 6, 7, or 8, further comprising:

adding error control information to the *data* sent over said link, wherein the error control information is added prior to transmitting the *data* over said link.

10. The method of claim 9, further comprising:
compressing the data prior to encrypting the data.

Because the parties essentially agree that the plain meaning of the disputed term should be applied, the Court need only resolve the two discrete issues of scope that the parties have presented. *See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) ("Claim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement. It is not an obligatory exercise in redundancy."); *see also O2 Micro*, 521 F.3d at 1362 ("[D]istrict courts are not (and should not be) required to construe every limitation present in a patent's asserted claims."); *cf. Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1207 (Fed. Cir. 2010) ("Unlike *O2 Micro*, where the court failed to resolve the parties' quarrel, the district court rejected Defendants' construction.").

In general, a limitation that is introduced by the definite article, "the," refers back to an earlier recitation of the limitation. *See, e.g., Process Control Corp. v. Hydreclaim Corp.*, 190 F.3d 1350, 1356-57 (Fed. Cir. 1999) ("It is clear from the language of the claim itself that the term 'a discharge rate' in clause [b] is referring to the same rate as the term 'the discharge rate' in clause [d].") (square brackets in original); *NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1306 (Fed. Cir. 2005) ("[I]t is a rule of law well established that the definite article 'the' particularizes the subject which it precedes. It is a word of limitation as opposed to the indefinite or generalizing force of 'a' or 'an.'") (quoting *Warner-Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1356 (Fed. Cir. 2003)). Plaintiff has failed to demonstrate why this general principle should not be applied to the disputed term in Claim 10, especially because "encrypting the data" and “decrypting the data” in Claim 1 can be readily understood to refer to all of the data that is recited as being transmitted. In order to resolve the parties’ dispute regarding the scope of Claim 10, the Court clarifies that “the data” refers back to all of the “data” introduced in Claim 1.

As to the compression function, however, Defendants themselves appear to agree with Plaintiff that Claim 10 is not limited to the use of a “single” compression function. Dkt. No. 87 at 29 (“The word ‘single’ does not appear in Defendants’ construction which instead refers to use of ‘a compression function.’”). Further, Defendants have not presented any dispute concerning the meaning constituent term “compressing,” so Defendants proposed reference to a “compression function” and to “reduc[ing] the size of the data” is unnecessary and would tend to confuse rather than clarify. Defendants’ proposed construction is therefore hereby expressly rejected.

The Court accordingly hereby construes **“compressing the data prior to encrypting the data”** to have its **plain meaning**, but the Court clarifies that “the data” in this term refers to all of the “data” introduced by recitation in Claim 1.

I. “each new key value in said [first] sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link” and “each new key value in said [second] sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link”

<table>
<tr><th colspan="2">“each new key value in said [first] sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link”</th></tr>
<tr><td><b>Plaintiff’s Proposed Construction</b></td><td><b>Defendants’ Proposed Construction</b></td></tr>
<tr><td>“a new key value in the first sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the transmitter”</td><td>“Defendants do not seek to have this term construed for these cases; Defendants contend that no construction of this term is necessary in view of the other constructions Defendants proffered.”</td></tr>
</table>

“each new key value in said [second] sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link”	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
“a new key value in the second sequence is produced each time a condition based on a predetermined characteristic of the transmitted data is met at the receiver”	“Defendants do not seek to have this term construed for these cases; Defendants contend that no construction of this term is necessary in view of the other constructions Defendants proffered.”

Dkt. No. 102, Ex. A at 3-4.

These terms appear as disputed terms in the parties’ post-briefing Joint Claim Construction Chart, but the parties presented no argument on these terms in their briefing. Also, in the parties’ pre-briefing Joint Claim Construction and Prehearing Statement, Defendants submitted that they “contend that no construction of the[se] terms is necessary in view of constructions proffered” for other terms. Dkt. No. 80, Ex. C at 14-15. In light of the absence of any substantive argument by the parties here, the Court concludes that these terms need not be construed.

CONCLUSION

Defendants' Emergency Motion to Strike Untimely Extrinsic Evidence (Dkt. No. 99) is hereby GRANTED.

The Court adopts the above constructions. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

SIGNED this 2nd day of December, 2013.

Roy S. Payne

ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE